**FAETERJ – RIO**

ARTHUR LOURENÇO MACHADO

JOÃO PEDRO DE FERREIRA OLIVEIRA FERREIRA

RODRIGO RODRIGUES FERREIRA MAGGESSI CASTRO

**DIFFIE-HELLMAN**

RIO DE JANEIRO

2022

ARTHUR LOURENÇO MACHADO - 1920478300009

JOÃO PEDRO DE FERREIRA OLIVEIRA FERREIRA - 2010478300069

RODRIGO RODRIGUES FERREIRA MAGGESSI CASTRO - 1910478300034

**DIFFIE-HELLMAN**

Trabalho de Segurança da Informação para a composição de nota da AV1 apresentado à FAETERJ-RIO.

Professora: Maria Cláudia Roenick.

**RIO DE JANEIRO**

**2022**

SUMÁRIO

[1. INTRODUÇÃO 4](#_Toc101884152)

[2. CRIPTOGRAFIA DIFFIE-HELLMAN 5](#_Toc101884153)

[3. FUNCIONAMENTO 6](#_Toc101884154)

[4. OPERAÇÃO COM MAIS DE DUAS PARTES 8](#_Toc101884155)

[5. AUTENTICAÇÃO E A TROCA DE CHAVES DIFFIE-HELLMAN 8](#_Toc101884156)

[6. VARIAÇÕES DA TROCA DE CHAVES E SUAS APLICAÇÕES 9](#_Toc101884157)

[Elliptic-curve Diffie-Hellman 9](#_Toc101884158)

[TLS 10](#_Toc101884159)

[ElGamal 10](#_Toc101884160)

[STS 11](#_Toc101884161)

[7. VANTAGENS E DESVANTAGENS DO ALGORITMO DIFFIE-HELLMAN 11](#_Toc101884162)

[8. CONCLUSÃO 12](#_Toc101884163)

[9. REFERÊNCIAS 13](#_Toc101884164)

1. INTRODUÇÃO

**Título:** Criptografia Diffie-Hellman

**Objetivo Geral:** A troca de chaves Diffie-Hellman é um método de troca segura de chaves criptográficas em um canal público e foi um dos primeiros protocolos de chave pública concebidos por Ralph Merkle e nomeados em homenagem a Whitfield Diffie e Martin Hellman. Será apresentado nesse trabalho toda a complexidade desse método, seu funcionamento, suas variações, vantagens e desvantagens.

2. CRIPTOGRAFIA DIFFIE-HELLMAN

Um dos principais problemas no uso da criptografia simétrica para a criação de um canal de comunicação segura é a troca de chaves, ou seja, o estabelecimento de um segredo comum entre duas pessoas.

A troca de chaves Diffie-Hellman é um método de troca segura de chaves criptográficas em um canal público e foi um dos primeiros protocolos de chave pública concebidos por Ralph Merkle e nomeados em homenagem a Whitfield Diffie e Martin Hellman. Tal conceito foi originalmente inventado por Malcolm Williamson, um funcionário do Government Communications Headquarters (GCHQ) no Reino Unido, alguns anos antes de Whitfield Diffie e Martin Hellman. Porém, o GCHQ decidiu não tornar pública a descoberta pois tratava-se de assunto de segurança nacional.

Em 2002, Hellman sugeriu que o algoritmo fosse chamado de chave de troca Diffie-Hellman-Merkle reconhecendo a contribuição de Ralph Merkle para a invenção da criptografia de chave pública.

O protocolo de Diffie-Hellman é baseado em aritmética inteira modular e constitui um exemplo bastante didático dos mecanismos básicos de funcionamento da criptografia.

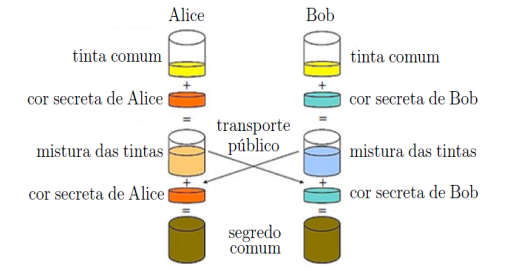


Figura 1. Diffie-Hellman é apresentado através de um esquema de cores.

3. FUNCIONAMENTO

A seguir segue um esquema prático de DH:

1. Alice e Bob entram em acordo para usar um número primo *p* = 23 e como base *g* = 5.
2. Alice escolhe um inteiro secreto ***a*** = **6**, e então envia a Bob A = *g****a*** mod *p*
   * A = 5**6** mod 23
   * A = **15.625** mod 23
   * A = 8
3. Bob escolhe um inteiro secreto ***b*** = **15**, e então envia a Alice B = *g****b*** mod *p*
   * B = 5**15** mod 23
   * B = **30.517.578.125** mod 23
   * B = 19
4. Alice calcula **s** = *B* ***a*** mod *p*
   * **s** = 19**6** mod 23
   * **s** = **47.045.881** mod 23
   * **s** = **2**
5. Bob calcula **s** = *A* ***b*** mod *p*
   * **s** = 8**15** mod 23
   * **s** = **35.184.372.088.832** mod 23
   * **s** = **2**
6. Alice e Bob compartilham agora uma chave secreta: **s** = **2**. Isto é possível porque 6\*15 é o mesmo que 15\*6. Alguém que tenha descoberto estes dois inteiros privados também será capaz de calcular s da seguinte maneira:
   * **s** = 5**6\*15** mod 23
   * **s** = 5**15\*6** mod 23
   * **s** = 5**90** mod 23
   * **s** = **807.793.566.946.316.088.741.610.050.849.573.099.185.363.389.551.639.556.884.765.625** mod 23
   * **s** = **2**

Tanto Alice quanto Bob chegaram no mesmo valor pois (*ga*)*b* e (*gb*)*a* são iguais mod *p*. Note que apenas *a*, *b* e *gab = gba* mod *p* são mantidos em segredo. Todos os demais valores – *p*, *g*, *ga mod p*, e *gb mod p* – são enviados limpos no canal público. Uma vez que Alice e Bob calculam a chave secreta, eles podem então usá-la como chave de encriptação, conhecida apenas por eles, para enviar e receber mensagens ao longo do mesmo canal de comunicação.

É claro que valores bem maiores de *a*, *b*, e *p* seriam necessários para tornar este exemplo seguro, uma vez que é fácil tentar todos os possíveis valores de *gab* mod 23. Existem apenas 23 possíveis inteiros que possuem os resultados observados para mod 23.

Por outro lado, se *p* for um primo de ao menos 300 dígitos e *a* e *b* tenham ao menos 100 dígitos, então até os melhores algoritmos conhecidos atualmente não poderiam encontrar *a* dado apenas *g*, *p*, *gb* mod *p* e *ga* mod *p*, mesmo usando todo o poder computacional existente na humanidade. Tal problema é conhecido como problema do logaritmo discreto. Note que *g* não precisa ser necessariamente grande, e na prática seus valores são usualmente 2 ou 5.

4. OPERAÇÃO COM MAIS DE DUAS PARTES

O acordo de chave Diffie – Hellman não se limita a negociar uma chave compartilhada por apenas dois participantes. Qualquer número de usuários pode participar de um acordo executando iterações do protocolo do acordo e trocando dados intermediários (que não precisam ser mantidos em segredo). Por exemplo, Alice, Bob e Carol podem participar de um acordo Diffie-Hellman da seguinte forma, com todas as operações consideradas como módulo *p* :

1. As partes concordam com os parâmetros *p* e *g* do algoritmo .
2. As partes geram suas chaves privadas, denominadas *a* , *b* e *c* .
3. Alice calcula *g a* e o envia para Bob.
4. Bob calcula ( g a ) b = *g ab* e o envia para Carol.
5. Carol calcula ( g ab ) c = *g abc* e usa-o como seu segredo.
6. Bob calcula *g b* e o envia para Carol.
7. Carol calcula ( g b ) c = *g bc* e o envia para Alice.
8. Alice calcula ( g bc ) a = *g bca* = *g abc* e usa-o como seu segredo.
9. Carol calcula *g c* e o envia para Alice.
10. Alice calcula ( g c ) a = *g ca* e o envia para Bob.
11. Bob calcula ( g ca ) b = *g cab* = *g abc* e usa-o como seu segredo.

Um intruso é capaz de ver *g a* , *g b* , *g c* , *g ab* , *g ac* e *g bc* , mas não pode usar nenhuma combinação deles para reproduzir com eficiência *g abc* .

5. AUTENTICAÇÃO E A TROCA DE CHAVES DIFFIE-HELLMAN

No mundo real, a troca de chaves Diffie-Hellman é raramente utilizada por si só. A principal razão por trás disso é que esse método não fornece autenticação. Isso deixa os utilizadores vulneráveis a ataques.

Estes ataques podem ter lugar quando a troca de chaves Diffie-Hellman é implementada por si só, porque não existem meios de verificar se a outra parte numa ligação é realmente quem diz ser. Sem qualquer forma de autenticação, os utilizadores podem estar de fato ligados a atacantes quando pensam estar se comunicando com uma parte de confiança.

Por esta razão, a troca de chaves Diffie-Hellman é geralmente implementada juntamente com alguns meios de autenticação. Isto envolve frequentemente a utilização de certificados digitais e um algoritmo de chave pública, como o RSA, para verificar a identidade de cada parte.

6. VARIAÇÕES DA TROCA DE CHAVES E SUAS APLICAÇÕES

A troca de chaves Diffie-Hellman pode ser implementada de várias maneiras diferentes e tem também fornecido a base para vários outros algoritmos. Algumas destas implementações fornecem autorização, enquanto outras têm várias características criptográficas, tais como o sigilo avançado perfeito.

Alguns protocolos que utilizam o algoritmo Diffie-Hellman para aumentar a segurança:

* **Secure Shell (SSH);**
* **Transport Layer Security (TLS)/Secure Sockets Layer (SSL);**
* **Infraestrutura de chave pública (PKI);**
* **Internet Key Exchange (IKE);**
* **Internet Protocol Security (IPSec).**

Elliptic-curve Diffie-Hellman

Elliptic-curve Diffie-Hellman aproveita a estrutura algébrica das curvas elípticas para permitir que as suas implementações atinjam um nível semelhante de segurança com um tamanho de chave menor. Uma chave elíptica-curva de 224 bits proporciona o mesmo nível de segurança que uma chave RSA de 2048 bits. Isto pode tornar as trocas mais eficientes e reduzir os requisitos de armazenamento.

Parte do comprimento menor da chave e o facto de confiar nas propriedades das curvas elípticas, a elliptic-curve Diffie-Hellman opera de forma semelhante à troca de chaves Diffie-Hellman padrão.

TLS

O TLS é um protocolo utilizado para proteger grande parte da Internet. Este utiliza a troca Diffie-Hellman de três maneiras diferentes: anônima, estática e efémera. Na prática, apenas a efémera deve ser implementada, pois as outras opções possuem problemas de segurança.

*Anonymous Diffie-Hellman* – esta versão da troca de chaves não utiliza qualquer autenticação, deixando-a vulnerável a ataques de man-in-the-middle. Não deve ser utilizada ou implementada.

*Diffie-Hellman Estático* – este utiliza certificados para autenticar o servidor.

*Diffie-Hellman Efémero* – esta é considerada a implementação mais segura porque fornece segredo forward perfeito. É geralmente combinado com um algoritmo, tal como DSA ou RSA para autenticar uma ou ambas as partes na ligação.

Diffie-Hellman efémero utiliza diferentes pares de chaves cada vez que o protocolo é executado. Isto dá à ligação um perfeito sigilo de avanço, porque mesmo que uma chave seja comprometida no futuro, não pode ser usada para decifrar todas as mensagens passadas.

ElGamal

ElGamal é um algoritmo de chave pública construído sobre a troca de chaves Diffie-Hellman. Tal como o Diffie-Hellman, não contém disposições para autenticação por si só, e é geralmente combinado com outros mecanismos para este fim.

ElGamal foi utilizado principalmente em PGP, GNU Privacy Guard e outros sistemas, porque o seu principal rival, RSA, foi patenteado. A patente da RSA expirou em 2000, o que lhe permitiu ser implementada livremente após essa data. Desde então, ElGamal não tem sido implementado com tanta frequência.

STS

O protocolo Station-to-Station (STS) também se baseia na troca de chaves Diffie-Hellman. É outro esquema de acordo chave, no entanto fornece proteção contra ataques de man-in-the-middle.

Requer que ambas as partes na ligação já tenham um par de chaves, que é utilizado para autenticar cada lado. Se as partes ainda não são conhecidas uma da outra, então os certificados podem ser utilizados para validar as identidades de ambas as partes.

7. VANTAGENS E DESVANTAGENS DO ALGORITMO DIFFIE-HELLMAN

**Vantagens:**

* O remetente e o destinatário não precisam de nenhum conhecimento prévio um do outro;
* Uma vez que as chaves são trocadas, a comunicação dos dados pode ser feita através de um canal seguro;
* O compartilhamento da chave secreta é seguro quando os elementos que compõem são escolhidos da forma correta.

**Desvantagens:**

* O algoritmo não pode ser processado por nenhuma troca de chaves assimétrica.
* Da mesma forma, não pode ser usado para assinaturas digitais.
* Como não autentifica nenhuma parte da transmissão, a troca de chaves de Diffie-Hellman é suscetível a um ataque do tipo Man-in-the-Middle.

8. CONCLUSÃO

Devido às suas vantagens, Diffie-Hellman provou ser um sistema útil de troca de chaves. Embora, seja realmente difícil de ser quebrado e um intruso espionar a rede, descriptografar os dados e obter as chaves, isso ainda é possível se os números gerados não forem inteiramente aleatórios e grandes o suficiente para impossibilitar a quebra por força bruta. Quando aliadas a outras técnicas de criptografia e segurança, Diffie-Hellman, se mostra bastante eficiente complementando um esquema de segurança de alta confiança.

9. REFERÊNCIAS

**- “Troca de chaves de Diffie–Hellman”. Wikipédia. Disponível em: <https://pt.wikipedia.org/wiki/Troca\_de\_chaves\_de\_Diffie%E2%80%93Hellman>. Acesso em: 21, abril de 2022.**

**- “Troca de chave Diffie-Hellman”. Stringfixer. Disponível em: <https://stringfixer.com/pt/Diffie-Hellman>. Acesso em: 21, abril de 2022.**

**- Ferreira, Thiago. “Algoritmo Diffie-Hellman”. iMasters, 2007. Disponível em: <** **https://imasters.com.br/back-end/algoritmo-diffie-hellman>. Acesso em: 20, abril de 2022.**

**- Marques, Thiago. “Criptografia: Abordagem histórica, protocolo Diffie-Hellman e aplicação em sala de aula”. Repositório UFPB, 2013. Disponível em: <** **https://repositorio.ufpb.br/jspui/bitstream/tede/7545/5/arquivototal.pdf >. Acesso em: 23, abril de 2022.**

**- “Algoritmo de Troca de Chaves de Diffie Hellman”. Education-wiki. Disponível em: <** **https://pt.education-wiki.com/4355142-diffie-hellman-key-exchange-algorithm>. Acesso em: 23, abril de 2022.**